Compliance Overview: **FISMA / NIST SP800-53**

Huntsman®
Defence-Grade Security Platform

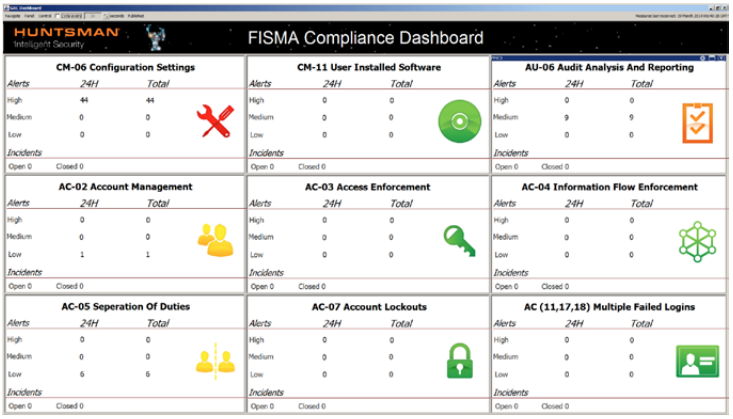
FISMA / NIST SP800–53: Compliance Overview

With Huntsman® SIEM

The US Federal Information Security Management Act (FISMA) is now a key element of the US Government's approach to the defense of its systems and information from a range of attacks and failure scenarios. Core to this is the role of the National Institute of Standards and Technology (NIST) that produces a range of documents that specify the risk management and control requirements and approaches.

NIST SPECIAL PUBLICATION 800–53 (SP800–53)

The standard, in its latest release, provides an approach to security and a catalogue of controls that support the mandatory FIPS Publication 200 (Minimum Security Requirements for Federal Information and Information Systems). Organizations define the security category of their systems using FIPS Publication 199 (Standards for Security Categorization of Federal Information and Information Systems). This results in an information system impact level that is then used to apply the appropriately tailored set of security controls in NIST SP800–531.



As such, the controls in SP800–53 form the basis of the overarching information, IT and cyber security defense posture. It represents the primary source of control selection within the US Federal Government and Defense environments, and also within the Critical National Infrastructure (CNI) community. SP800–53 categorizes controls under the following families:

ID	Family	ID	Family	ID	Family
AC	Access Control	IA	Identification & Authentication	PS	Personnel Security
AT	Awareness and Training	IR	Incident Response	RA	Risk Assessment
AU	Audit & Accountability	MA	Maintenance	SA	System & Services Acquisition
CA	Security Assessment & Authorization	MP	Media Protection	SC	System & Communications Protection
CM	Configuration Management	PE	Physical & Environmental Protection	SI	System & Information Integrity
CP	Contingency Planning	PL	Planning	PM	Program Management

HUNTSMAN®: SUMMARY OF NIST SP800–53 COMPLIANCE OVERVIEW

This overview focuses on the ways in which an environment that requires compliance to SP800–53 needs to implement a comprehensive security monitoring and incident management regime; and specifically it shows how Huntsman® forms the hub of a security ecosystem that enables this. It should be read in conjunction with Huntsman's more in-depth Compliance Mapping Guide that provides greater detail for compliance managers.

AC — Access Control

Huntsman supports the following requirements in this section: AC–2, 3, 4, 5, 6, 7, 11, 17, 18, 19, 20, 16

Huntsman® collates event and activity data related to authorization, access control and account management. It provides a central repository for analysis, rule-based alerting, behavioral anomaly detection, reporting and storage that allows networks, platforms, applications and information systems to direct their automatically generated audit information relating to account creation, modification, enabling, disabling, and removal to a single managed location.

Huntsman® provides specific queries that focus on access controls and account management activities at the user and systems level that track this activity and report on the identity of the person/account making changes; as well as the subject. It captures the access logs pertaining to files, applications, resources and information systems for successes and failures that can be used to verify correct operation of systems and controls and provides specific queries to track object and system accesses made by users – both failures (indicating misuse or attempts to gain access) and successes.

Huntsman®'s powerful alerting facilities enable it to generate alerts relating to particularly risky scenarios, such as connections from certain geographies, successes and failures, abnormal flows/volumes of network traffic or onward connections to sensitive systems from remote access users. This would include specified access control issues around segregation of duties and identity.

AU — Audit and Accountability

Huntsman supports all requirements in this section: AU–1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

Huntsman® directly supports an organization's defined audit policy. It enables the definition of individual operational responsibilities and access rights to data and functionality across the security operations team at all stages of the detection and incident response process. Huntsman® collects, stores and processes log data centrally, away from the system or platform where it is generated to avoid a malicious administrator or hacker from covering their tracks by removing the audit information that contains their session activity.

At the core of this process, Huntsman® detects threats, manages security incidents and generates reports and summaries to the relevant stakeholders. Huntsman®'s correlation and alerting engine, behavioral anomaly detection and advanced threat intelligence capabilities relate usage logs to multiple risk adjusted factors and threat information. It provides a fully customizable reporting engine and extensive library of inbuilt queries, allowing effective oversight, operational management and reporting; thus leveraging the information collected for audit, compliance and policy reporting purposes. This enables Huntsman® to analyze and correlate seemingly unrelated events to determine any suspicious activities that threaten the information assets and systems of the organization.

Huntsman® systematically collects and retains detailed logs of security operator activities as part of this process so they are readily available for regular and independent review and audit.

Huntsman enables the security operations / investigation team to answer difficult questions like "Who was responsible?", "What data has been exposed?", "Where has it gone to?", "What can we do about it?" when breaches do occur.

CA — Security Assessment and Authorization

Huntsman supports the following requirements in this section: CA–2, 3, 7

Huntsman® integrates security assessment information from leading vulnerability management systems to ensure that risk profiles and log data can be effectively corroborated. This facility allows Huntsman® operators to cross-reference up to date vulnerability and risk information resulting from security assessment and scanning activity. Huntsman® fulfills a vital role in tracking usage, monitoring network flows, traffic and connections; and it can detect failures or breaches using its correlation engine, or where the user or system behavior itself can be detected as anomalous and flagged to a security operator.

CM — Configuration Management

Huntsman supports the following requirements in this section: CM–3, 5, 6, 11

Huntsman® monitors logs for signs of activity that could indicate changes, modifications, reconfigurations or software installation. For example, information derived from logs pertaining to privilege assignment or authentications, from direct changes to systems, data, applications or configuration, or as a result of the cryptographic file integrity monitoring features that Huntsman® provides. It enables real-time alerting when suspicious incidents or actual breaches occur and the ability to reconcile activity of administrators to planned and expected changes or to the investigation of known incidents.

IA — Identification and Authentication

Huntsman supports the following requirements in this section: IA–2, 3, 8

Huntsman® collects and processes the authentication and access logs from systems themselves or dedicated authentication servers such as two-factor authentication systems to provide a full alerting capability around authentication failures or suspicious behavior such as brute force attacks. This gives a point of reference for the audit of system user accounts (and new device connections) to ensure that new users have not been wrongly created and that appropriate authorization processes have been followed. The inbuilt queries and reporting capabilities provide information around user accesses, logins, failures and connection of new devices and systems across a variety of system, user management and network environments.

IR — Incident response

Huntsman supports the following requirements in this section: IR–4, 5, 6

Huntsman® is a full-featured security event and information management solution; but it goes beyond this to deliver a complete Incident Management capability. Once an incident has been flagged within the log, event or activity data; through Behavioral Anomaly Detection (BAD) or by an analyst; Huntsman® enables organizations to manage the full analysis, containment and recovery process – tied into the role based access control model, fully audited, and with excellent workflow and reporting capability for compliance and security managers.

When incidents are detected they can be directed to appropriate personnel for investigation. A full incident summary can be generated at any time and reports around incident statuses can be generated on an ad hoc basis or according to a pre-defined schedule.

MA — Maintenance tools

Huntsman supports the following requirements in this section: MA–3, 4, 5

Monitoring maintenance, support and service activities centrally within Huntsman® ensures that even where the origin of a support activity or remote administration is external to the organization, outside its physical or network boundary or being undertaken by a third party, there is a robust record of the access and changes made to ensure this falls within known/planned changes or ongoing incidents.

MP — Media protection

Huntsman supports the following requirements in this section: MP–7

Huntsman® reports on detection and use of media, devices, remote storage and USB connections – either directly (from logs pertaining to device connection or driver installation) or through integration with endpoint protection or data loss prevention (DLP) solutions.

PE — Physical And Environmental Protection

Huntsman supports the following requirements in this section: PE–6

Huntsman® can be linked to physical security controls around buildings, computer rooms or other secure areas. It can achieve this either by receiving the turnstile or swipe card access logs, or using status information as to physical location or building presence of staff, coupled with IT logs to derive meaningful attack warnings where anomalous situations arise. For example, a user connecting to an internal network when they are not currently in the building indicating the use of shared accounts or tailgating.

PS — Personnel security

Huntsman supports the following requirements in this section: PS–4, 5

Huntsman® ensures changes to accounts, addition or deletion of users and changes to group memberships can be centrally tracked and reported on. This means that when a user is leaving the organization or changing role/department, the records of their various accounts being disabled and terminated can be easily and centrally generated – enabling leavers processes to be reconciled against the accounts they were known to have held and identifying any deviation between access that had been granted, and that which has not been removed.

Huntsman® provides the capability to automatically gain additional levels of monitoring over staff who are in the process of leaving; for example through the creation of a set of "Departing Users" within the solution which would enable any anomalous flows of data, email activity or system access to be flagged and treated as significant.

SC — System and Communications Problems

Huntsman supports the following requirements in this section: SC–5, 7, 8, 15, 18, 19, 26, 32

Huntsman® utilizes its behavioral anomaly detection engine to help provide early warning of external denial of service (including distributed denial of service) attack scenarios. Due to its placement 'out-of-band' away from the systems themselves, it also provides a useful point for investigation and resolution; where live systems are failing or slow to respond, the log and activity data captured by Huntsman® will be the best source of diagnostic information in terms of events just before problems were noted, and events during the attack itself.

Huntsman® collects data from the security systems that enforce network defenses between organizations and the wider Internet or third parties. This includes firewalls, proxies, network devices, IDS and IPS solutions, VPN gateways, data loss prevention (DLP) solutions and wireless devices. Correlating this information centrally enables Huntsman® to use the event data from all these platforms to swiftly detect attacks; and to provide a unified audit trail, through its queries and reports, of the true nature of the situation to investigators.

SI — System and Information Integrity

Huntsman supports the following requirements in this section: SI–3, 4, 7, 12

Organizations typically have a range of security controls. Huntsman® provides a single consolidated point where these various controls can be aggregated to gain a unified picture of viruses and malware defenses, reports and outbreaks. Without a single, centralized monitoring platform in place like Huntsman® security operators often struggle to match up activity,outbreak information and manage incidents across the different product silos.

As a technologically advanced, and fully capable and scalable SIEM solution, Huntsman® provides comprehensive systems event, security and activity monitoring as well as more general capabilities around systems monitoring, log data collection and retention. Huntsman® interfaces with other enterprise solutions to support systems and network performance monitoring, support and fault management, and configuration and asset management. Its distributed data model allows event and activity information in the primary database to be aged and archived to a set of fully accessible and queryable secondary database systems to enable the use of cheaper hardware and storage technologies.

Huntsman® addresses the challenge of compliance with an intelligent, centralized approach; it integrates with existing security solutions, network devices and IT systems, creating a single, holistic monitoring system.

Huntsman® enables organizations to capture, analyze and report on events anywhere in the environment, as they occur as part of a fully comprehensive threat and incident management workflow. Achieving compliance with Huntsman® provides clear visibility, reporting and assurance to technicians, senior management stakeholders and auditors alike.

BROADER BENEFITS OF SEAMLESS COMPLIANCE

In addition, using its patented behavioral technology BAD 2.0, Huntsman® identifies suspicious activity, human or IT-related, within any dataset, providing unique insights to risk as well as compliance.

Huntsman®:

- Monitors access to key IT assets in real-time;
- Monitors activity at the enterprise boundary and within it;
- Detects & alerts to suspicious or risky activity across the organization; and
- Prevents the loss of valuable or sensitive information such as IP or personnel records

Huntsman® delivers integrated, effective protection through continuous monitoring of your ICT assets with timely alerts of suspicious, risky or non-compliant activity. This way, you always know who is accessing and using your systems, applications and data, what they are doing with them, where they are taking them and whether the activity is legitimate or not.

Huntsman® is proven in mission-critical environments; securing defense, government, intelligence and corporate environments worldwide. These enterprises chose Huntsman® because its superior technology enables their compliance today, and ensures they can adapt quickly to changing compliance and security requirements in the future.

Huntsman | Tier-3 Pty Ltd

Asia Pacific

t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

North Asia

t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

Americas

toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman